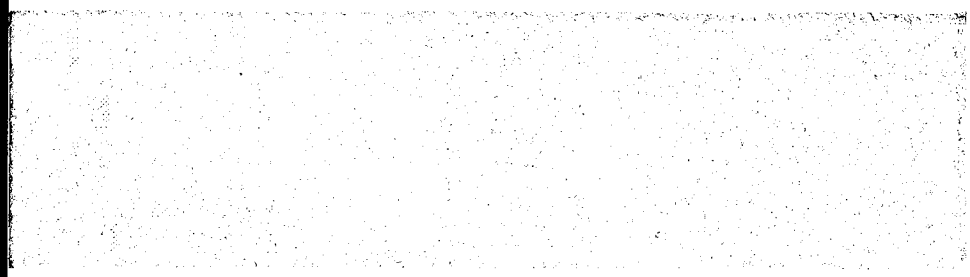

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035-1000

ARC 275 (Rev Mar 93)

RNS-90-001

Password Security In a Large Distributed Environment

Michele D. Crabb
Computer Sciences Corporation*
NASA Ames Research Center
Moffett Field, CA 94035

ABSTRACT

With the increased interest in, or rather need for, better security in UNIX† computing environments, password security and control is one issue which must be addressed completely. In the past, when a single VAX 11/780‡ serving 30 users was the status quo, password security was simple in that a system administrator merely had to remember a few privileged passwords and ensure that all user accounts had passwords. However, in today's large-scale environments where central support of 100 or more systems is common and with the availability of fast password cracking programs, password security has become a complex issue. Password security no longer involves just remembering the root password for a particular system or ensuring all accounts have passwords. It now involves the concept of using "smart" passwords, management of a large number of privileged passwords and a equally large number of people who need access to those passwords, and a much tighter control on who has access to the *root* and other privileged accounts.

This paper will examine the current methods used for password security and control at the Numerical Aerodynamic Simulation (NAS) facility at NASA-Ames Research Center. The NAS environment consists of over 170 systems running the UNIX operating system with the TCP/IP network protocol software which supports over 1000 users nationwide. On-going support and software development for NAS is provided by close to 150 personnel. Due to the large number of systems, users and support personnel, implementing password security and control at NAS has been a challenging task.

Some specific topics that will be discussed are: the concept of "special access" accounts; how password groups and levels of access are defined; the formal NAS policies concerning access to privileged accounts; how all the information regarding the numerous privileged passwords is tracked and recorded; and one alternative to providing the *root* password to everyone who needs root access.

---

* This work is supported by contract NAS2-12961 of the National Aeronautics and Space Administration to Computer Sciences Corporation.

† UNIX is a registered trademark of AT&T.

‡ VAX is a trademark of Digital Equipment Corporation.

1.0 Introduction

The Numerical Aerodynamic Simulation (NAS) facility, which supports over 1000 users nationwide, is composed of over 170 computer systems running some version of the UNIX operating system with TCP/IP network protocol software. These systems are interconnected into a heterogeneous network using various types of networking hardware. Ongoing support and software development for the NAS facility is provided by close to 150 personnel. Due to the nature of their responsibilities, many of these people require access to the privileged accounts on one or more of the NAS systems. With numbers such as these, it becomes quite apparent that password security [1] and control in a large environment like NAS can be a challenging task.

This paper will discuss the methods currently used for providing password security and control for special accounts such as the *root* account. The notion of a "special access account" is defined along with policies governing such accounts. A step-by-step description of a "day in the life of a password change at NAS" is provided and one alternative to sharing of the *root* password is examined. Some ideas for the future improvements to password security are also presented.

2.0 A Brief Look into the Past

Up until three or four years ago, password security at NAS was lax at best. The environment was more of the type found in a small university than in a national supercomputing center. No one person had knowledge of all the people who had access to the *root* account on the various systems. If a person needed the *root* password for a certain system, he/she simply asked around until a person was found who knew the *root* password. During this time, it was also common to have *root* passwords that were not known by anyone. Use of *root* ***/.rhosts*** files was widespread; therefore, if the *root* password was not known for a particular system, you merely had to remotely log in from another system where the *root* password was known. Periodic password changes were also a rare event. When the *root* passwords were changed, people were not notified in any formal manner. If a person discovered the password had changed, he/she would ask a system analyst or control room analyst for the new password.

As the number of NAS systems and users increased, password security started to become an issue. Primitive methods for tracking *root* passwords across all NAS systems were put into place. One early solution to the problem was to use the **crypt (1)** command to encrypt an ASCII file which contained all of the *root* passwords. Then, instead of giving out the individual passwords, the key used to encrypt the file was given out. However, this method was vulnerable to attacks due to the weaknesses of the **crypt (1)** command and the availability of the "Cryptographer's Workbench" package [2]. As time passed, password security slowly increased to its current level, which will be described in the remainder of this paper.

3.0 Password Security for Special Access Accounts

Before discussing password security for special access accounts, I need to first define what is meant by a special access account and provide a brief description of the NAS system support and administration philosophy. A "special access" account is defined to be any account required for the support of the NAS facility and whose password is centrally controlled. A special access account may be shared by numerous support personnel or not shared at all. Any person who has the password and privilege to use one of the special access accounts is considered to have "special access."

3.1 The NAS Support Philosophy

The philosophy for system support at NAS is probably much like many large computing environments. To facilitate support of NAS systems, the different branches of the NAS Systems Division are subdivided into "subsystems" based on computer architecture or type of support (i.e., on-going vs. development). Some of the current subsystems are: Workstation subsystem (WKS), High Speed Processor subsystem (HSP) and Data Communication Network Support subsystem (DCN).

Support responsibilities are aligned via the different subsystems in the NAS Systems Division. Generally, there will be one Lead System Analyst (LSA) and one or more support personnel providing system administration and software development in any one

subsystem. A LSA or support analyst for one subsystem does not have any authority to make changes on a system in another subsystem, even if that person has *root* privilege on the other system. A minimum requirement for each support person is to have access to any privileged account on the systems within their area of responsibility. Some people provide support in multiple areas and thus require a wider range of special access. For example, Control Room Analysts are responsible for front line support of all NAS systems and must have access to all special access accounts.

3.2 Password Groups and Levels of Access

At NAS just keeping tabs on the *root* passwords for all systems and who has access to these passwords is a major task. Throw in an additional dozen or so special access accounts which may be on one or all NAS systems and you have one major password security headache. To simplify the task of maintaining *root* passwords on 180 plus systems, NAS has had to do away with some of the traditional rules governing *root* and other special account passwords. At NAS we use the concept of password groups where systems with similar support status and/or of similar architecture are named as a password group and share a common *root* password. For example, all fully supported production file servers would share a common *root* password referred to as the "Sun FS" password. All fully supported production workstations (there are three architectures in this group) would share a common *root* password called "WKS Pro."

Password groups are only used for groups of systems which are supported by people who can have access on all systems in the password group. Therefore, if a group of systems is supported by two or more people who do not have access to all privileged accounts on those systems, each system would be required to have a separate *root* password. Furthermore, any system which cannot be classified into one of the common support classifications will have a unique *root* password. Shared support accounts, such as a printer administration account, would have a common password across all NAS systems.

Closely related to password groups for systems are the levels of access for support

groups. Most support groups at NAS are aligned with a NAS subsystem (i.e., WKS support group, VAX support group, HSP support group). In order to reduce the amount of special access required by system support personnel, a minimum baseline of special access groups for individual support groups has been established. In other words, for any one support group, there is a baseline group of special access passwords required by all members of the support group. For example, all members of the HSP support group need access to the *root* account on all HSP production systems and the HSP gateway systems. There are some support groups which require access to the *root* account on every system at NAS, due to the scope of their responsibilities. The Network Support Group and the Control Room Analysts are two such groups.

3.3 Policies Concerning Special Access Accounts

Due to the increasing number of people with special access at the NAS facility, it was necessary to establish a policy concerning access to special (or privileged) accounts. The policy provides a set of requirements for the regulation and use of special access on the NAS systems. The policy also provides procedures for the addition and removal of people from the special access database and a mechanism for periodic reviews of the special access database.

Part of implementing the policy on special access was developing a separate form to request special access and writing a set of rules concerning the do's and don'ts of special access. The Special Access Request form requires users to justify their need for such access and it requires management signatures at three levels. On the form is a small set of basic rules governing special access. Persons requesting special access must sign the form certifying that they will abide by all rules and regulations concerning special access.

The special access form documents the "who, what, when, where and why" of special access for each user and serves as a helpful document for future reference. The "who" is the person requesting special access. The "what" is the type of special access they are requesting. The "when" is the date they were granted special access and the date that

their special access expires or must be re-justified. The "where" is the system(s) on which they have requested special access. The "why", the most important of the five, is the user's justification for needing special access. Prior to the implementation of the special access policy, little justification was required when requesting access to privileged accounts. As a result, many people had access to accounts for which they had no justification or need.

The full set of rules concerning special access is documented separately and is referred to as the "Special Access Guidelines Agreement." The agreement lists some general guidelines as well as some specific do's and don'ts governing the use of special access. The main motivation for the Special Access Guidelines Agreement was to help people use their special access in a responsible and secure manner. The agreement also provides a handy reference point for those abusers of special access who use the excuse "they did not know better."

Some of the "do's" listed in the agreement are:

1) Be aware of the NAS environment.
2) If possible, log on to a system as yourself and then "su" to the needed UID.
3) Use special access only if necessary.
4) Document all major actions.
5) Have a backup plan in case something goes wrong.

Some of the specific "don'ts" listed in the agreement are:

1) Do not share special access passwords with anyone.
2) Do not write down the passwords or current algorithm.
3) Do not read or send personal E-mail, play games, read the net news or edit personal files using a special access account.
4) Do not browse or alter other users' files.

3.4 Tracking the Information

By now it should be apparent that there is a lot of information to store and to track. Just trying to remember all of the password group names can be as difficult as trying to

remember the actual passwords, or the names of all the people with special access. Obviously, this is an area where a database is needed. At NAS, all of the password information is stored in a HyperCard database on a MacIntosh* diskette, which is kept under lock and key. Information stored in the database includes: names of special access groups, all current passwords and passwords for the last three months, and the full names and login IDs of all support personnel with special access.

For each support person there is associated a "card." The information contained on each card is the user's full name, the user's login ID, the contact person (for off-site employees), the current date, and list of password groups for which the user has been granted access. In addition to user cards, there are also password cards. Each password card contains a table of all password groups with the appropriate password for each group. A new password card is created each time the passwords are changed, which provides an audit trail of previous passwords used. Each time a new user or new password group is added to the database, a new list of users with special access is created. This list, called the "sulist," is a quick reference of who has access for what group of systems.

3.5 The Use of Password Sheets

Aside from the large amount of information which must be stored, a major motivation for implementing a password database was to facilitate the printing of "password sheets." Due to the large number of password groups, it is necessary to provide support personnel with a small sheet of paper which lists all of the passwords for which they have been granted access. Even if every person was able to remember up to 40 different passwords, there would still be the dilemma of informing 85 or more people each time the passwords are changed. The natural solution seemed to be to provide each person with their personal list of passwords which they could carry on their person.

The password sheet currently provided is small enough to fit in an ID badge envelope

---

* HyperCard and MacIntosh are trademarks of Apple Computer Corporation.

which can be worn along with the other NAS badges. Since the implementation of password sheets, the task of informing everyone of a password change has been reduced to having users come pick up their new password sheets when they need them. Even though the use of password sheets seems to nullify one of the major concepts of password security, it has served NAS well over the past three years.

To offset some of the dangers of having passwords documented on a sheet of paper, NAS has implemented the concept of using a password algorithm. A password algorithm is some function to be applied to the password written on the password sheet to get the actual password. So, in reality, the passwords are not written down verbatim. For example, on the password sheet the password listed for system "A" might be "freem3" and the algorithm might be "capitalize the first vowel and add a dash "-" to the end." Then the actual password for system "A" would be "frEem3-." The password algorithm is not to be written down, thus allowing NAS to meet two of the normal security validation checks. At NAS we can verify "what you have," which is the password as written on the password sheet. We can verify "what you know," which is the password algorithm needed to obtain actual passwords. But unfortunately, we cannot verify "what you are" with the current technology[3].

3.6 A Day In The Life of A Password Change

Special access passwords are changed on a periodic basis. The passwords are split into two major change groups - quarterly and monthly. Passwords for systems and/or accounts which are shared by a small group of people (< 10) are changed on a quarterly basis. All other passwords are changed on a monthly basis. The password algorithm is changed on a quarterly basis.

Given the large number of special access password groups, the very large number of systems at NAS and the number of people who receive special access passwords, the periodic change of passwords is not a trivial exercise. The entire exercise takes several days to complete and must be treated with care so as not to disclose the new passwords or to interrupt system service because a password was changed without notifying the

appropriate people. The task can be broken down into several steps.

The first, and most interesting part of the process is to create new passwords. Password construction rules for special access accounts at NAS are: passwords must be at least eight characters long; passwords must have mixed case, at least one decimal number and they must have one special character. The password construction rules apply to the final password after the password algorithm has been applied. Therefore, the passwords listed on the password sheet may not conform to all of the above construction rules. An example of a NAS password, as listed on the password sheet, is "freem3" and the actual password, after applying the algorithm, is "frEem3-."

Once the passwords are created, the special access database is updated and the new password sheets are printed. The password sheets must either be printed in a secure area or on a printer that someone is monitoring during the entire print job. After all password sheets have been printed and cut to size, a notification is sent, via E-mail to all people with special access. The notification must be sent out a minimum of eight hours in advance and preferably 24 hours before the actual password change occurs.

After the notification has been sent out, people may pick up their new password sheets which are available in the Control Room. All local support personnel are required to sign for their password sheet and may only pick up the sheet belonging to them. Personnel who provide support from a remote site have a local point-of-contact person who picks up and signs for their password sheet. The point-of-contact will then provide the password over the phone, to the remote support personnel, but only when needed. Members of the control room staff are responsible for ensuring that each support person only picks up and signs for his/her password sheet.

The final stage of the task is to manually change the passwords on each system. Passwords are always changed during the second and third shift of the day. A checklist is provided to the people responsible for actual password changes and as each password is changed on a particular system, the person changing the password initializes the checklist for that system. All systems where passwords were not changed

during the first pass, due to some problem such as a down system, are retried the next morning. If there are still systems where the password could not be changed for one reason or another, the problem is passed off to the LSA for that system.

3.7 Dealing with Special Access Problems

Just as with any situation where you have a large number of objects and a large group of people interacting with those objects, there are bound to be problems. Special access on NAS systems is no exception. Although NAS has experienced very few problems concerning special access passwords, problems do occur on occasion and need to be addressed. The most common problem seems to be a lost password sheet. Lost password sheets are supposed to be reported to the security analyst within 24 hours. If the password sheet was lost in the vicinity of Ames (i.e., where someone is likely to recognize the system names), then the passwords will be changed that same day. Otherwise, if the sheet was lost in a "relatively" benign area or sent through the washer in a shirt pocket, a new sheet will be printed for the person who lost it and the passwords will remain unchanged.

Another problem concerning special access passwords is the termination (friendly or otherwise) of an employee who has special access. If the person with special access is leaving NAS on a friendly basis, the password will be changed within five working days, or during the next regular change of passwords. However, if the person is leaving under unfriendly circumstances, all passwords and the algorithm will be changed that same day. Major violations of special access by a given individual may also result in changing all passwords for which the individual had access. A major violation would be something along the lines of deliberately destroying system or user files.

4.0 Other Issues

4.1 The Use of Root */.rhost* Files

In general, the use of *root /.rhost* files at NAS is not recommended or even allowed. However, there are several justifiable uses for the *root /.rhost* file. One such area is on

the NAS workstations. There are currently over 150 workstations at NAS of different architectures and/or operating system revisions. One of the main tools used by the workstation support group to maintain these systems is the **rdist (1)** command. In order to use **rdist (1)** effectively, the NAS workstations must trust *root* "r-commands" from a few selected workstations which serve as binary baseline systems [4]. However, in 98% of the cases, the trust is not bi-directional (i.e., System A may trust *root* from System B, but not vice versa).

Another possible justification for the use of *root* ***/.rhost*** files would be for remote boots of diskless workstations over the network. In general, NAS does not support diskless workstations; however, there are a few occasions when a system must be remotely booted over the network. Once the system has been booted, the ***/.rhost*** entry for the boot server would be removed. Root ***/.rhosts*** files have also been used on the VAX systems to allow remote dumps when a tape drive is down. However, once the tape drive is restored, the ***/.rhosts*** entry will be removed.

4.2 LSU - An alternative to sharing the *root* password

The use of non-unique *root* passwords does present a small problem from time to time. Some users or support personnel will need access to the *root* account on their personal workstation which may be part of a password group. However, it may be the case that management does not wish to provide the individual with *root* access to all workstations in the password group. As an alternative, such users are given *root* access on their systems via the **lsu (1L)** command. Lsu is a a local super-user program written by Matt Bishop [5]. However, I must state that Matt does not recommend using the **lsu (1L)** command to provide *root* access for people.

The **lsu (1L)** command works much in the same manner as the **su (1)** command; however, the password expected is that of the invoking account and not the target account. A configuration file must specify who can use the **lsu (1L)** command and what accounts they can switch to. Use of the **lsu (1L)** command can be restricted to time of day, day of week, month of year and terminal line or dial-up line.

Lsu access is not given out freely. People requesting *root* access, via **lsu (1L)** on a single system must have a good justification for needing the access and they must possess enough knowledge of the UNIX operating system to know what to do and what not to do. Weekly audits are run on the **lsu** configuration files to ensure the files have not been modified. Any system which allows **lsu** access to one or more persons cannot be listed in a *root* ***/.rhosts*** file on any NAS system. In addition to the restriction of ***/.rhosts*** files, the password files on all systems are audited nightly for changes using the **getall (8 L)** command [6], so any change made to a password file will be reported the next day. To date, there have been VERY few problems with using the **lsu (1L)** command to provide *root* access on individual workstations.

5.0 The Future of Special Access Password Security

There are several things that could be done to improve the current level of password security for special access accounts at NAS. The biggest gains could be realized by automating the process of changing passwords. The task of manually changing two or more special access passwords on 180 plus systems is very time consuming and error prone. Ideally, NAS would like to have a secure network administration tool that could change passwords on multiple systems without sending the clear text password over the network. If such a tool were available, the processes to change passwords could be batched and verified ahead of time and then "let loose" when the right time approached. Another area of improvement would be the automatic generation or assignment of passwords. For example, a database could be populated with a year's supply of passwords. At each password change, the new passwords could automatically be assigned to each password group. Reducing the number of password groups would also provide some relief from having to remember numerous passwords; however, this scenario is not likely to be achieved at NAS. Another, perhaps more drastic, means of increasing special access password security would be to reduce the level of privileges for people with special access.

6.0 Summary

This paper has presented the methods used for password security and control at the NAS facility, which can be viewed as a typical large distributed computing environment. Due to the number of systems and the nature of services provided by the NAS facility, password security and control has been a challenging task. The current method which involves the use of password groups, minimum levels of access, a MacIntosh database and printed password sheets has served NAS well over the past several years. However, as the number of NAS systems continues to increase, improvements such as an network password changing utility or even a whole new method, will need to be implemented.

Acknowledgments: Thanks to Bob Van Cleef and Bill Wall for their helpful reviews of the earlier drafts of this paper.

References

[1] Grampp, F.T. and Morris, R.H., "Unix Operating System Security," AT&T Bell Laboratories Technical Journal, 63, 8 (October 1984) 1649 - 1672.

[2] Baldwin, R. W. "Crypt Breakers Workbench," *baldwin@xx.lcs.mit.edu*, October 1986, USENET posting.

[3] Anderson, L. E., "UNIX Password Security," In Proceedings of the USENIX Security Workshop, August 1988, p 7.

[4] Van Cleef, R. E., "System Administration and Maintenance of Fully Configured Workstations," In Proceedings of the USENIX System Administration of Large Scale Installations Conference, November 1988.

[5] Bishop, M., "Collaboration Using Roles," Software – Practice and Experience, vol. 20, no. 5, pp. 485-497 (May 1990).

[6] Van Cleef, R. E., *getall.* NASA, NASA Ames Research Center, Moffett Field, CA., March 1990, private communications.